Computer & Communications Industry Association
Tech Advocacy Since 1972

February 25, 2019

The Honorable Janice D. Schakowsky
Chairwoman
Subcommittee on Consumer Protection & Commerce
Committee on Energy & Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Cathy McMorris Rodgers
Ranking Member
Subcommittee on Consumer Protection & Commerce
Committee on Energy & Commerce
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairwoman Schakowsky and Ranking Member McMorris Rodgers:

On behalf of the Computer & Communications Industry Association (CCIA), I write regarding the Subcommittee's hearing on "Protecting Consumer Privacy in the Era of Big Data." CCIA is an international association that represents companies of all sizes in the high technology products and services sectors, including in computer hardware and software, electronic commerce, telecommunications, and Internet products and services.[1]

This hearing is timely, and CCIA appreciates the Subcommittee's efforts to examine these critical issues. Public attention to the subject of data protection, risks of the emergence of an unworkable 50-state patchwork of inconsistent regulations, and pressures from international privacy frameworks, such as the General Data Protection Regulation (GDPR), have underlined the need for strong and consistent rules of the road for the treatment of consumer information. In November 2018, CCIA issued its "Privacy Principles: A New Framework for Protecting Data and Promoting Innovation," setting out principles for federal action that would ensure that data is handled responsibly and transparently while also ensuring that individuals can benefit from innovation and new technologies.[2] These principles are attached for your reference. A growing number of companies, trade associations, and civil society groups also support the development of strong, baseline federal privacy legislation in order to promote a sustainable digital economy that will drive U.S. innovation and competitiveness. CCIA has created a chart organizing various industry proposals and highlighting the key issue areas they have addressed.[3]

[1] CCIA's members employ more than 750,000 workers and generate annual revenues in excess of $540 billion. A full list of CCIA members is available at https://www.ccianet.org/members.

[2] *Privacy Principles: A New Framework for Protecting Data and Promoting Innovation*, Computer & Commc'ns Indus. Ass'n (Nov. 2018), http://www.ccianet.org/wp-content/uploads/2018/11/CCIA_Privacy_Principles.pdf.

[3] *See Envisioning a Federal Baseline Privacy Framework*, Disruptive Competition Project (Feb. 25, 2019), https://www.project-disco.org/privacy/022519-envisioning-federal-baseline-privacy-framework/.

**GAO Report**

CCIA welcomes the Government Accountability Office's (GAO) recent privacy report to Chairman Pallone,[4] which recommends that Congress "consider developing comprehensive legislation" on privacy and raises three issues for Congressional consideration. CCIA supports the thrust of the GAO report toward comprehensive, baseline federal legislation to protect consumer privacy without disrupting existing federal, sector-specific frameworks. However, legislation with a limited scope could undermine widely shared goals. The goal of baseline federal rules should be to ensure that individuals can expect consistent treatment of their personal information throughout the economy. Rather than artificially limiting new legislation to "Internet privacy," a new framework should apply to all organizations that collect and process personal information, including both online and offline companies, whether or not they have a direct commercial relationship with consumers. CCIA offers the following comments on three important questions posed by the GAO.

Which agency or agencies should have oversight?

Comprehensive baseline privacy legislation should be primarily enforced by the Federal Trade Commission (FTC) and extend uniformly to businesses and non-profit organizations. The FTC has experience and expertise in the data privacy and security context. The FTC's existing privacy authority allows it to bring enforcement actions against "unfair and deceptive acts and practices in commerce" and enforce a variety of sector-specific laws such as the Children's Online Privacy Protection Act (COPPA).[5] The FTC may bring enforcement actions to require companies to take affirmative steps to remediate unlawful behavior. These actions have included mechanisms such as requiring the implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, and providing robust transparency and choice mechanisms to consumers.[6]

What authorities should a regulating agency have?

As the GAO report recommends, it is appropriate to consider granting APA-rulemaking authority to the FTC to implement a suitably specific baseline privacy law. It is also appropriate to consider whether the FTC should have the authority to issue civil penalties to first-time violators of that law. However, these proposals should not be the boundaries of the conversation over federal privacy authority.

Congress should evaluate whether State Attorneys General should be empowered to investigate when the FTC has declined to act. Congress should also provide the FTC with additional resources and staffing to conduct investigations, take enforcement actions, host workshops, issue public reports, and complete the necessary empirical studies to quantitatively evaluate the net consumer benefits and harms of particular

[4] U.S. Gov't Accountability Office, GAO-19-52, Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility (Jan. 15, 2019), https://www.gao.gov/assets/700/696437.pdf.

[5] 15 U.S.C. §§ 6501–6506.

[6] *Privacy & Data Security Update: 2017*, Fed. Trade Comm'n (Jan. 18, 2018), http://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf.

business practices to ensure that its regulatory approach is grounded in facts. While the U.S. economy has become increasingly data driven, the FTC's budget has declined an estimated five percent over the course of this decade.[7] The FTC should be given more authority to police consumer privacy, but it cannot achieve this mission without sufficient funding or personnel.

How can regulators balance consumers' privacy goals with business innovation?

CCIA supports the GAO's recognition that regulations must be balanced with organizations' needs to provide services and to pursue socially beneficial innovation. Overly broad or prescriptive regulatory requirements would create significant overhead costs and record-keeping demands on small companies and raise the barriers to entry for new market players. Privacy legislation should, therefore, set baseline requirements, while providing industry with flexibility in meeting those requirements. Requirements should also be scalable based on context, such as organizations' scale and resources, and the sensitivity and uses of that data at issue. Finally, enforcement should account for and be proportionate to the risk of harm caused by noncompliant practices.

Federal baseline privacy legislation should be rooted in the Fair Information Practice Principles (FIPPs), which are at the heart of global privacy regimes worldwide and have proven to be flexible and durable over time. In addition to robust enforcement carried out by the FTC, appropriately balanced federal baseline privacy legislation should be characterized by extensive transparency requirements and meaningful consumer controls. Organizations should be transparent about what data they are collecting, how they are using it, and when and why data may be transferred to third parties. Consumers should also have the right to object to data processing where feasible, and to reasonably access, correct, and request the deletion of their personal information. Entrenching these rights and obligations through a baseline privacy law will allow consumers to exercise greater choice and control in the digital economy, promote competition on privacy within industry, and preserve American innovation and competitiveness.

**Conclusion**

We look forward to working with you and other stakeholders on a strong and flexible modern privacy framework for the digital economy. Thank you again for holding today's important hearing.

Sincerely,

Edward J. Black
President & CEO
Computer & Communications Industry Association

[7] John A. Howes, Jr. & Jacqueline Yin, *Comments of CCIA before NTIA on Developing the Administration's Approach to Consumer Privacy*, Computer & Commc'ns Indus. Ass'n (Nov. 7, 2018), http://www.ccianet.org/wp-content/uploads/2018/11/CCIA-NTIA-Privacy-Comments.pdf.

Computer & Communications Industry Association
Tech Advocacy Since 1972

# PRIVACY PRINCIPLES:

## A New Framework for Protecting Data and Promoting Innovation

## Purpose

As the world becomes increasingly data-focused, attention has inevitably shifted to the impact of data on consumers and whether and how improvements should be made. Recent controversies have shifted how companies and consumers think about how data is collected and used online, generating some positive responses in terms of practice and transparency. It is important for the U.S. to have a healthy data ecosystem with transparency and accountability, which will help drive innovation and U.S. competitiveness.

CCIA supports the development of baseline, Federal privacy legislation that would ensure that data is handled responsibly and with transparency while also ensuring that individuals can benefit from innovation and new technologies. Such a framework should be technology-neutral, meaning it should not provide specific technology mandates; sector-neutral, meaning it should apply to online and offline organizations; and it should provide for safe harbors and flexibility for organizations to make adjustments according to the needs of individuals and evolving technology. CCIA presents these "Privacy Principles" to help guide the development of a national policy on consumer privacy.

## Policy Overview

These principles aim to protect data through a robust, technology-neutral framework for assessing and managing privacy risks to individuals and organizations, and to promote innovation, in both digital services and privacy protection. Organizations across the digital ecosystem use personal data to provide innovative services. Responsible data use can be beneficial for people, businesses, and society. Reasonable data protection measures that align with individuals' expectations can protect people and communities from harms that result from misuse of data and help maintain the trust that enables the digital economy.

CCIA | 655 15th St NW #410 | Washington, DC 20005 | ccianet.org | Phone: +1 (202) 783-0070 | Fax: +1 (202) 783-0534

When evaluating the reasonability of an organization's data protection practices, it is important to understand the context in which an organization collects, processes, and uses personal information. This context can include the nature of the relationship between an individual and the organization; the potential benefits an individual, organization, and society might receive from particular uses of information; and individuals' expectations regarding data protection.

Individuals depend on organizations to use their data responsibly and be transparent about what they are collecting and how they are collecting and using it. Therefore, organizations must respect individuals' interests when they process personal information. Organizations should make reasonable best efforts to account for and mitigate potential harms to individuals, communities, and society.

## Scope and Definitions

**Personal information or data** include any data under the control of a covered organization, that is not de-identified or otherwise generally available to the public through lawful means, and is linked or practically linkable to a specific individual, or linked to a specific device or account that is associated with or routinely used by an individual.

Different types of personal data can vary in sensitivity, depending on the context. However, some personal data is almost always sensitive. This includes data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation, and certain data of known minors.

**Privacy risk**
The potential for personal information, on its own or when linked to other information that might identify an individual, to cause economic loss, discrimination, exclusion, loss of self determination, or physical, reputational, or professional harm to an individual.

**Covered organizations or entities** include all organizations that process personal information regardless of whether they have a direct or commercial relationship with an individual whose information they hold.

**Proportionality**
Reasonable data protection practices may differ across covered organizations. Context, including an organization's scale and resources, the sensitivity of the data it holds, and its uses for that data, should inform the measures that it puts in place to protect data.



CCIA | 655 15th St NW #410 | Washington, DC 20005 | ccianet.org | Phone: +1 (202) 783-0070 | Fax: +1 (202) 783-0534

**Interoperability**
Cross-border data flows are essential to the modern economy. Organizations and individuals benefit from consistent compliance programs based on widely shared principles of data protection. These principles are intended to be interoperable and consistent with existing cross-border data transfer mechanisms, industry standards, and other cross-organization cooperation mechanisms.

## Requirements for Organizations

**Control**
Covered organizations must provide appropriate mechanisms for individual control, considering the service. Individuals should be able to object to data processing where it is feasible, but specific consent should not be mandatory for every aspect of data processing, which could create an overly complex and confusing experience for the individual and divert from the overall goals that the policy seeks to achieve. Policymakers should also keep in mind that the responsible processing of personal information is necessary to simply operate some services.

**Access**
Individuals must be able to access the personal information that they have provided to a covered organization, and it should be made available for export in a machine-readable format.

**Accuracy**
Personal information should be accurate, current, and complete to the extent possible for the purpose for which the covered organization maintains the data.

**Deletion**
Pursuant to the above "Access" principle, covered organizations should afford users with the ability to correct and/or delete the data that they provide to that organization when it would be practical and provided that deletion would not implicate the personal information of others.

**Portability**
Covered organizations should make reasonable efforts to enable authenticated users to obtain data they provide to that organization for their own purposes or for use with a different organization or service, provided that these data portability tools do not implicate the personal information of others. Data transfers between covered organizations should be private, secure, and balanced. Data portability tools should: (1) allow users to download and move data they have provided to the service, but not data that may relate to other users; (2) afford users control over how and when the tools are used; and (3) be tailored to the privacy and security expectations of specific products and services. Further, data portability tools should enable machine-to-machine transfers where technically feasible.



CCIA | 655 15th St NW #410 | Washington, DC 20005 | ccianet.org | Phone: +1 (202) 783-0070 | Fax: +1 (202) 783-0534

**Security and Integrity**
Users should expect that organizations handling their data will do so carefully and responsibly with reasonable measures to protect personal information from unauthorized access, misuse, modification, disclosure, loss, and destruction. Policy should account for and be proportionate to the risk of harm. Organizations should follow consensus best practices, and if a security breach occurs, organizations should notify individuals expeditiously when there is a significant risk of harm.

**Onward Transfers**
Covered organizations should ensure that personal information that they collect or process is protected in a manner consistent with the above principles even if it is transferred to third parties. Covered organizations should use enforceable mechanisms and independent audits to ensure that third parties protect data according to these principles.

## Accountability

**Transparency**
Covered organizations must be transparent about the types of personal information that they are collecting and how they are collecting and using it. Covered organizations should be clear about whether the personal information may be transferred to third parties, how long information may be retained, and what choices and controls individuals have with respect to their personal information. Covered organizations should make reasonable efforts to actively inform individuals, making the information relevant and actionable, about data use in the context of the relevant services.

**Accountability**
Covered organizations should be held accountable for meeting the requirements set out in these Privacy Principles. Covered organizations should regularly assess the privacy risks associated with their collection, processing, and use of personal information; develop systems to mitigate risks in a reasonable and proportionate manner; and monitor services for bias and disparate impacts. Organizations should practice privacy by design, building products and services that prioritize privacy, security, reliability, and reduce the likelihood of vulnerabilities, which will help earn user trust. Policymakers should set baseline requirements but enable flexibility to meet those requirements and promote industry accountability programs and safe harbors.

**Enforcement**
A robust federal baseline would provide clear standards for covered organizations and ensure that individuals across the United States can expect consistent data protections from organizations that retain their data. A national, privacy framework should be consistent throughout the United States, so state laws concerning data privacy, security, and breach notifications should be preempted where appropriate. This framework should be enforced primarily by the FTC at the federal level, but it should allow for enforcement by state attorneys general where the FTC has declined to act.



CCIA | 655 15th St NW #410 | Washington, DC 20005 | ccianet.org | Phone: +1 (202) 783-0070 | Fax: +1 (202) 783-0534